

# Guided Specification and Analysis of a Loyalty Card System

Laurent Cuennet<sup>1</sup> Marc Pouly<sup>2</sup> **Saša Radomirović<sup>3</sup>**

<sup>1</sup>University of Fribourg

<sup>2</sup>Lucerne University of Applied Sciences

<sup>3</sup>Institute of Information Security, ETH Zürich

July 13, 2015



HOCHSCHULE  
LUZERN

**ETH** zürich

# Loyalty Cards



Paper-based ink stamp cards are a convenient and inexpensive way for small shops to improve customer loyalty.

- ▶ Advantage: customer benefits without being tracked and profiled.
- ▶ Disadvantage: too many different cards accumulate over time.

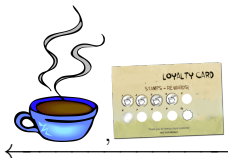
# Physical Loyalty Card Protocol



Customer



Vendor



# Sketch of Electronic Loyalty Card Protocol



Mobile



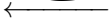
Customer



Vendor



Server



# Security Requirements



**Customer anonymity:** Vendor cannot link points to customer's identity.

**Customer privacy:** Vendor cannot link customer's transactions.



# Security Requirements



**Customer anonymity:** Vendor cannot link points to customer's identity.

**Customer privacy:** Vendor cannot link customer's transactions.

**Theft protection:** Points issued to an agent can be redeemed by the agent.

# Security Requirements



**Customer anonymity:** Vendor cannot link points to customer's identity.

**Customer privacy:** Vendor cannot link customer's transactions.

**Theft protection:** Points issued to an agent can be redeemed by the agent.

**Non-repudiation:** Vendor cannot repudiate validity of unredeemed points.

# Security Requirements



**Customer anonymity:** Vendor cannot link points to customer's identity.

**Customer privacy:** Vendor cannot link customer's transactions.

**Theft protection:** Points issued to an agent can be redeemed by the agent.

**Non-repudiation:** Vendor cannot repudiate validity of unredeemed points.



**Unforgeability:** Loyalty points accepted by vendor have been issued by vendor.

**No double-spending:** Redeemed loyalty points will not be accepted.



# Security Requirements



**Customer anonymity:** Vendor cannot link points to customer's identity.

**Customer privacy:** Vendor cannot link customer's transactions.

**Theft protection:** Points issued to an agent can be redeemed by the agent.

**Non-repudiation:** Vendor cannot repudiate validity of unredeemed points.



**Unforgeability:** Loyalty points accepted by vendor have been issued by vendor.

**No double-spending:** Redeemed loyalty points will not be accepted.

## Theft protection

Points issued to an agent can be redeemed by the agent:

- ▶ “Agent” = Mobile Device.

We are not protecting against theft of Mobile Device.

# Theft protection

Points issued to an agent can be redeemed by the agent:

- ▶ “Agent” = Mobile Device.

We are not protecting against theft of Mobile Device.

## 2 Threats:

1. Points issued to a mobile device are redeemed by an attacker's device.  
⇒ Requirement: Confidentiality of loyalty points.
2. Points issued to a mobile device are corrupted or lost and thus not redeemable by the device.  
⇒ Requirement: Authenticity of loyalty points.

# Theft protection

Points issued to an agent can be redeemed by the agent:

- ▶ “Agent” = Mobile Device.

We are not protecting against theft of Mobile Device.

## 2 Threats:

1. Points issued to a mobile device are redeemed by an attacker's device.  
⇒ Requirement: Confidentiality of loyalty points.
2. Points issued to a mobile device are corrupted or lost and thus not redeemable by the device.  
⇒ Requirement: Authenticity of loyalty points.

**Remaining Problem:** Transmit Loyalty Points from Server to Mobile Device authentically and confidentially.

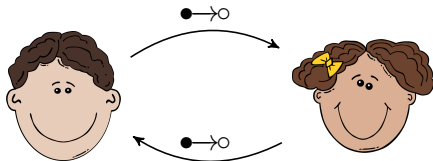
# Communication Topology [BRS15]



What assumptions can we make about

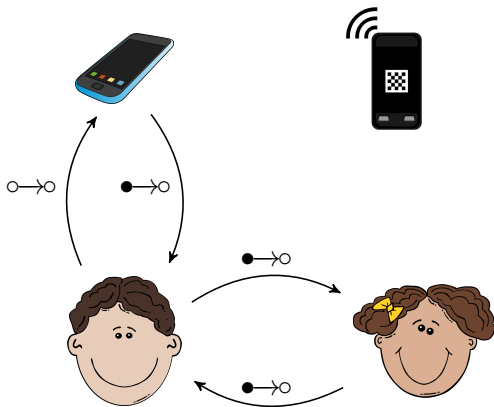
- ▶ the **communication channels** between the four parties?
- ▶ the **capabilities** of the four parties?
- ▶ the **honesty** of the four parties?

# Communication Channels



Authentic Channel between Customer and Vendor, due to context and location.

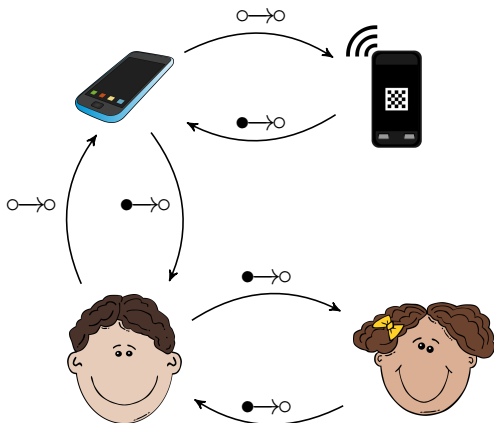
# Communication Channels



Authentic Channel from Device to Customer: Customer knows his device.

Insecure Channel from Customer to Device: Anybody could input information into Device.

## Communication Channels

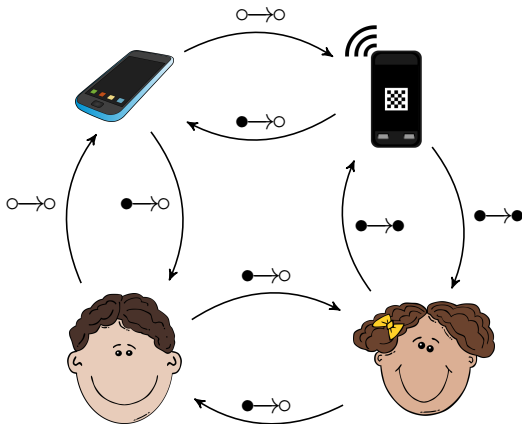


Insecure Channel from Device to Server: Any Device can send information to Server.

Authentic Channel from Server to Device: Server's public key can be distributed authentically in the shop.

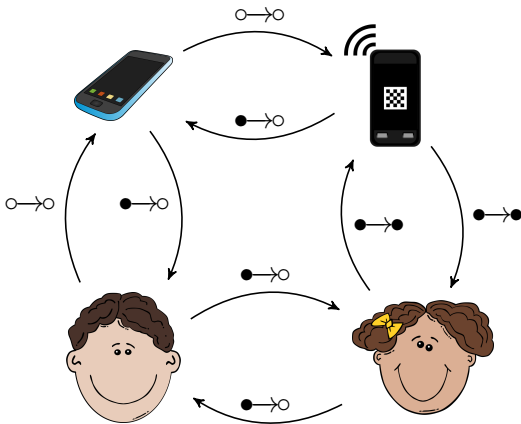


# Communication Channels



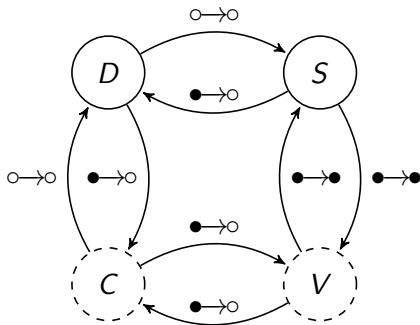
Secure Channel between Vendor and Server due to physical access control.

# Honesty and Capabilities



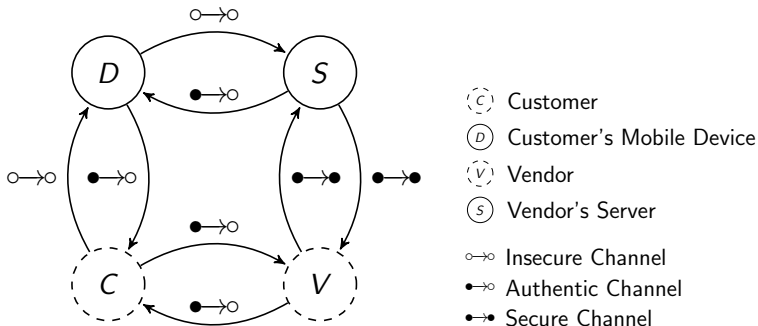
- ▶ We assume all four agents are honest.
- ▶ Customer and Vendor are computationally restricted.

# Coffee Shop Topology



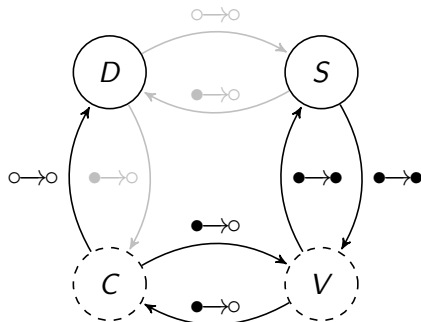
- (C) Customer
- (D) Customer's Mobile Device
- (V) Vendor
- (S) Vendor's Server
- Insecure Channel
- Authentic Channel
- Secure Channel

# Coffee Shop Topology



How to transmit Loyalty Points from Server *S* to Mobile Device *D*  
**authentically** and **confidentially**?

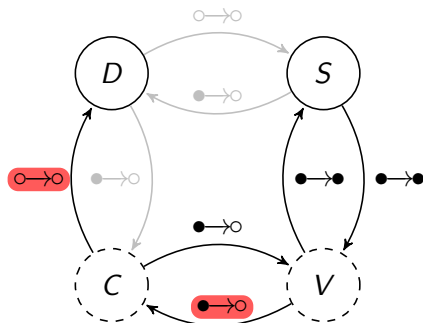
# First Protocol



1.  $C \rightarrow V$ : money
2.  $V \rightarrow S$ : money
3.  $S \rightarrow V$ : points / QR
4.  $V \rightarrow C$ : QR
5.  $C \rightarrow D$ : QR / points

Are the points transmitted from  $S$  to  $D$  confidential?

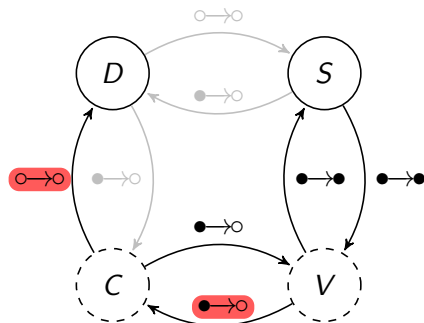
# First Protocol



1.  $C \rightarrow V$ : money
2.  $V \rightarrow S$ : money
3.  $S \rightarrow V$ : points / QR
4.  $V \rightarrow C$ : QR
5.  $C \rightarrow D$ : QR / points

Are the points transmitted from  $S$  to  $D$  confidential? - **No!**

# First Protocol

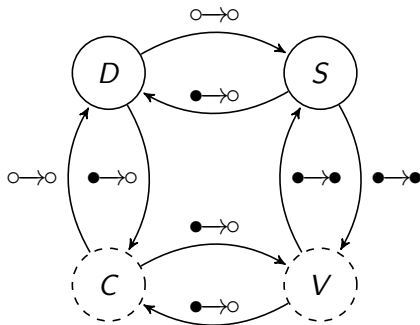


1.  $C \rightarrow V$ : money
2.  $V \rightarrow S$ : money
3.  $S \rightarrow V$ : points / QR
4.  $V \rightarrow C$ : QR
5.  $C \rightarrow D$ : QR / points

Are the points transmitted from  $S$  to  $D$  confidential? - **No!**

Options: (1) Change assumptions, (2) Improve protocol.

## Second Protocol

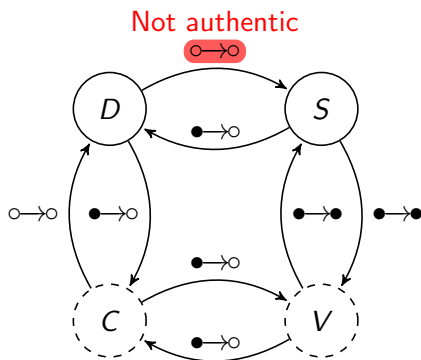


- ?  $D \rightarrow S$ : **key**
- 1.  $C \rightarrow V$ : money
- 2.  $V \rightarrow S$ : money
- 3.  $S \rightarrow V$ :  **$\{\text{points}\}_{\text{key}}$**  / QR
- 4.  $V \rightarrow C$ : QR
- 5.  $C \rightarrow D$ : QR /  **$\{\text{points}\}_{\text{key}}$**

► **Idea:**  $S$  encrypts points for  $D$ . Server needs a key for  $D$ .



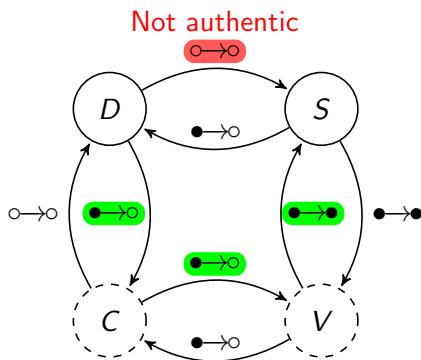
## Second Protocol



- ?.  $D \rightarrow S$ : **key**
1.  $C \rightarrow V$ : money
2.  $V \rightarrow S$ : money
3.  $S \rightarrow V$ :  **$\{\text{points}\}_{\text{key}}$**  / QR
4.  $V \rightarrow C$ : QR
5.  $C \rightarrow D$ : QR /  **$\{\text{points}\}_{\text{key}}$**

- ▶ **Idea:**  $S$  encrypts points for  $D$ . Server needs a key for  $D$ .
- ▶ **Problem:** How to send information authentically from  $D$  to  $S$ ?

## Second Protocol

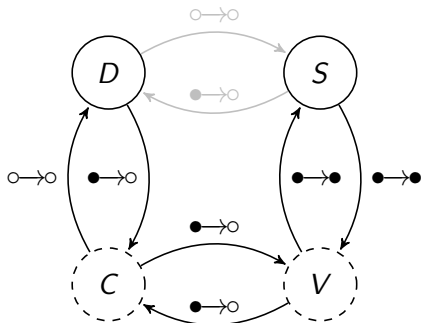


- ?.  $D \rightarrow S$ : key
1.  $C \rightarrow V$ : money
2.  $V \rightarrow S$ : money
3.  $S \rightarrow V$ :  $\{\text{points}\}_{\text{key}}$  / QR
4.  $V \rightarrow C$ : QR
5.  $C \rightarrow D$ : QR /  $\{\text{points}\}_{\text{key}}$

- ▶ **Idea:**  $S$  encrypts points for  $D$ . Server needs a key for  $D$ .
- ▶ **Problem:** How to send information authentically from  $D$  to  $S$ ?

Information can be sent authentically along path  $[D, C, V, S]$ .

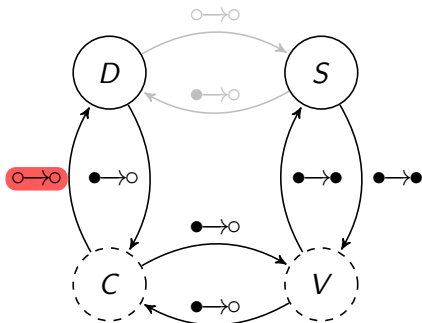
## Second Protocol



1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow V$ :  $\{\text{points}\}_{\text{key}}$  / QR
6.  $V \rightarrow C$ : QR
7.  $C \rightarrow D$ : QR /  $\{\text{points}\}_{\text{key}}$

Are the points transmitted from  $S$  to  $D$  authentic?

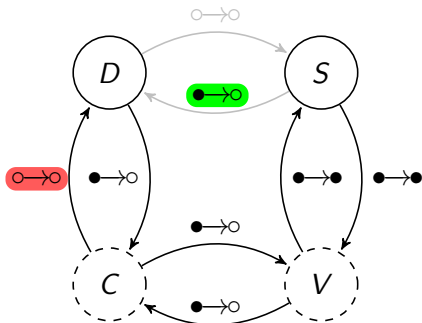
## Second Protocol



1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow V$ :  $\{\text{points}\}_{\text{key}}$  / QR
6.  $V \rightarrow C$ : QR
7.  $C \rightarrow D$ : QR /  $\{\text{points}\}_{\text{key}}$

Are the points transmitted from  $S$  to  $D$  authentic? - No!

## Second Protocol

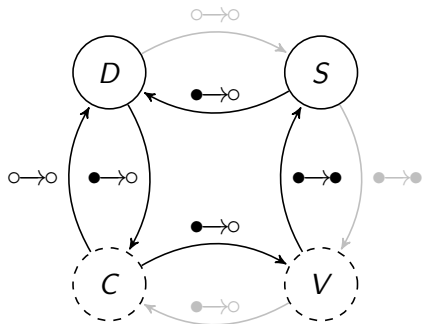


1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow V$ :  $\{\text{points}\}_{\text{key}}$  / QR
6.  $V \rightarrow C$ : QR
7.  $C \rightarrow D$ : QR /  $\{\text{points}\}_{\text{key}}$

Are the points transmitted from  $S$  to  $D$  authentic? - **No!**

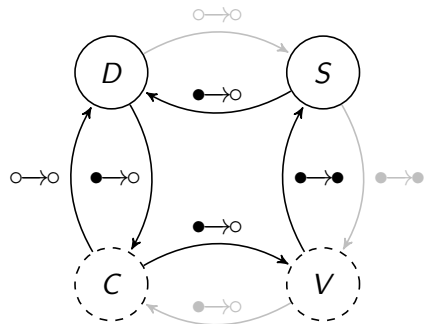
Idea: Use authentic channel  $S \bullet \rightarrow \circ D$  to transmit  $\{\text{points}\}_{\text{key}}$ .

## Third Protocol



1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow D$ :  $\{\text{points}\}_{\text{key}}$

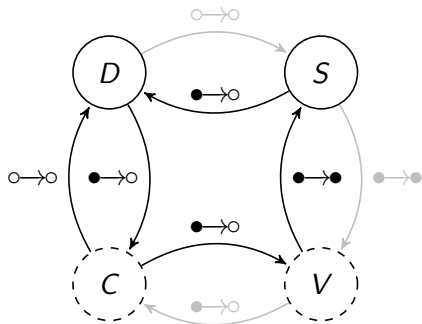
## Third Protocol



1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow D$ :  $\{\text{points}\}_{\text{key}}$

- ▶ We have modeled the protocol with the Tamarin prover.
- ▶ Tamarin verifies authenticity and confidentiality for points transmitted from  $S$  to  $D$ .

## Third Protocol



1.  $C \rightarrow D$ : GetPoints
2.  $D \rightarrow C$ : key
3.  $C \rightarrow V$ : money, key
4.  $V \rightarrow S$ : money, key
5.  $S \rightarrow D$ :  $\{\text{points}\}_{\text{key}}$

- ▶ We have modeled the protocol with the Tamarin prover.
- ▶ Tamarin verifies authenticity and confidentiality for points transmitted from  $S$  to  $D$ .
- ▶ It does not satisfy the privacy requirement: Vendor can link points redeemed to purchases.  
See paper for a solution based on an e-cash scheme.



## Conclusion



- ▶ We have introduced the coffee shop topology and used it to design a novel security protocol.
- ▶ The security protocol exemplarily designed is a light-weight electronic customer loyalty program that improves upon commercially deployed systems.
- ▶ Our example illustrates the use of communication topologies to guide the design of security protocols.
- ▶ This approach helps to quickly rule out insecure protocol designs and thus to reduce the protocol designer's search space.

## Future Work

- ▶ Interactive and automated protocol design:

What is the “most secure” communication channel achievable for a given arbitrary communication topology?

How to automatically construct the corresponding protocol?



# Future Work

- ▶ Interactive and automated protocol design:

What is the “most secure” communication channel achievable for a given arbitrary communication topology?

How to automatically construct the corresponding protocol?

- ▶ Refined set of channels: ●→●, ●→●, 👤→🖨️, 📞→👤

E.g.: Human-computer interface is different from network links.

- ▶ More general attacker model.



## Future Work

- ▶ Interactive and automated protocol design:

What is the “most secure” communication channel achievable for a given arbitrary communication topology?

How to automatically construct the corresponding protocol?

- ▶ Refined set of channels: ●→●, ●→●, 👤→🏠, 📞→👤

E.g.: Human-computer interface is different from network links.

- ▶ More general attacker model.
- ▶ Light-weight loyalty point system that supports collaborating shops or franchises.

# Questions?



## References:

[BRS15] David Basin, Saša Radomirović, and Michael Schläpfer.  
*A Complete Characterization of Secure Human-Server  
Communication.* (CSF 2015).

[R15] Tamarin specification files:  
[www.infsec.ethz.ch/research/projects/hisp.html](http://www.infsec.ethz.ch/research/projects/hisp.html)